2024 年４月 30 日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第６回会合の議事概要

１．開催要領

（日時）2024 年３月 25 日（月）14 時 00 分～16 時 00 分
（形式）対面形式およびＷｅｂ会議形式
（参加者）別紙のとおり

２．プレゼンテーション

セコム株式会社、株式会社ゆうちょ銀行よりプレゼンテーションが行われた。概要は以下のとおり。

（１）当人認証の現状および最新動向の整理①（セコム株式会社）

―― プレゼンテーション資料は別添１を参照。

当人認証を議論する上で必要と思われる概念や用語の整理および、最新動向の紹介、ならびにＣＢＤＣの検討における課題・論点を説明する。

本人確認や身元確認、当人認証といった言葉はこれまでの会合でも出ているが、局面によって使われ方が異なる場合があるため、本プレゼンでは経済産業省の「オンラインサービスにおける身元確認手法の整理に関する検討報告書」にならい、「本人確認」は「身元確認」と「当人認証」の２つの要素で構成されているという整理のもと説明を行う。その他の用語や概念は、米国のＮＩＳＴ（Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄｓ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ）が制定するガイドライン「ＮＩＳＴ ＳＰ８００－６３」を参考に整理する。なお、当人認証を議論する上では、同一単語で複数の意味を持つ用語や、和訳が混同する用語も多く存在するため、注意が必要である。

まず、サービス申込からサービス利用までの一般的なフローと付随する脅威を整理する。フロー全体を俯瞰すると、①取引時確認、②登録、③当人認証、④サービス機能の利用、の順となる。①取引時確認では、本人確認資料の提示

等により、ユーザーの身元確認が行われ、②登録で、認証手段（ＩＤ・パスワード等）の設定や、身元確認を行ったユーザーと認証器（スマートフォン等）との紐付けが行われる。③当人認証では、②で登録した認証手段・認証器を用いて、ユーザー当人であることが確認され、その後に④サービス機能の利用となる。なお、異なるシステム間で当人認証結果の伝達・連携を行うＩＤ連携は③の当人認証に含まれる。また、③の認証手段は、「知識（Ｓｏｍｅｔｈｉｎｇ　ｙｏｕ　ｋｎｏｗ）」、「所持（Ｓｏｍｅｔｈｉｎｇ　ｙｏｕ　ｈａｖｅ）」、「生体認証（Ｓｏｍｅｔｈｉｎｇ　ｙｏｕ　ａｒｅ）」の３要素に分類できる。

そして、①～③で考えられる脅威だが、①取引時確認では、本人確認資料の偽造や、容姿・容貌を偽る人物偽装等によるなりすましが考えられる。②登録では、身元確認を行ったユーザーと攻撃者の認証器との不正な紐付けが考えられる。これは、初回の登録以降、認証器の紛失、機種変更等に伴う認証器とユーザーの再紐付け（再登録）を行う際の方法が万全でない場合に発生しうる不正であるが、その方法はサービス提供事業者ごと異なることから、ガイドライン等でカバーされていない範囲で、事業者ごとに登録時のフローの設計や運用を行うために脆弱性が生まれやすいポイントとなっており注意が必要である。③当人認証では、キーロガーなどのマルウェアによるＩＤ・パスワードの不正取得や認証器自体の窃盗等による認証器への攻撃や、ユーザーとサービス間の通信の盗聴・改ざん・再送攻撃等による認証プロトコルへの攻撃、フィッシング・リアルタイムフィッシングといったサービスのなりすまし等によるサービスへの攻撃等の脅威が考えられる。また、ＩＤ連携時には、ＩＤ連携元サービスとＩＤ連携先サービスとの身元確認、当人認証レベルが異なる場合、その相違を利用した不正等も発生しうる。

脅威への対策には、脅威とそのリスクを分析した上で、適切な対策の設計／選定・実装が必要であり、その際には、ＦＩＤＯ２．０や、Ｏｐｅｎ　ＩＤ　Ｃｏｎｎｅｃｔ等の標準規格や、ＮＩＳＴのＳＰ８００－６３等のガイドラインを可能な限り活用することが望ましいと考える。ただし、標準規格やガイドラインが解決しようとしている課題を理解した上で、適切に実装・運用することが重要であり、この点は、ＣＢＤＣの検討でも同様であると考える。

続いて、新たな技術動向として２点紹介する。１つ目は、「Ｄｉｇｉｔａｌ　Ｉｄｅｎｔｉｔｙ　Ｗａｌｌｅｔ」。スマートフォンなどの端末で、自らの身元を示す身元確認情報や属性情報、資格等が管理可能なウォレットのことで、ＥＵが技術指標を定め、ＥＵ加盟国がウォレットを作成する構図となっている。２つ目は、「Ｖｅｒｉｆｉａｂｌｅ　Ｃｒｅｄｅｎｔｉａｌｓ」。証明書の非改ざん性を維持しつつ、ユーザーの意思によって開示できる情報をコントロールできるデジタル版の証明書で、身分証明や属性証明等に使用できる。

以上を踏まえ、ＣＢＤＣにおける論点を３点挙げる。まずは、「標準化・ガイドライン」である。ＣＢＤＣのユースケースやシステムモデルを整理しつつ、各ケースでどのような標準化やガイドラインが必要かを議論する必要があると考える。例えば、当人認証においては、認証手段や認証器に対する保証レベルの整理が必要と考える。次に、「プライバシー保護」も重要な論点として挙げる。ＣＢＤＣにおけるユーザー情報や利用履歴についてのプライバシー保護はとても大事である一方、ＡＭＬ／ＣＦＴの観点から不正利用等があった際に、追跡できるような仕組みも必要と考えられ、プライバシー保護とＡＭＬ／ＣＦＴに関してどのようなバランスで設計するかは議論が必要と考える。最後に、「短期的／中長期的な視点での技術動向の追従」を挙げる。短期的な視点は今まさに直面している脅威にどのように対応するかという点、中長期的な視点は新たな技術に関して将来的な導入も視野に入れた上での計画立案が必要であるという点であり、これらをどのように実現していくかは議論が必要と考えている。

（２）当人認証の現状および最新動向の整理②（株式会社ゆうちょ銀行）

――　プレゼンテーション資料の要旨は別添２を参照。

当人認証を取り巻く状況、当行の取組、ＣＢＤＣの検討課題を実務の観点から説明する。

当人認証のガイドラインが国内外で整備されているが、足許では不正利用の手口巧妙化やＩＴ技術革新等を踏まえて、各種ガイドラインの改定が図られている。デジタル庁による「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」、ＯｐｅｎＩＤファウンデーション・ジャパンによる「民間事業者向けデジタル本人確認ガイドライン」、ＮＩＳＴによる「ＳＰ８００－６３」等の見直しが進められており、フィッシング耐性を高めることが主な要点として挙げられている。米国のＣＩＳＡ（Ｃｙｂｅｒｓｅｃｕｒｉｔｙ ａｎｄ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ Ｓｅｃｕｒｉｔｙ Ａｇｅｎｃｙ）の「Ｉｍｐｌｅｍｅｎｔｉｎｇ Ｐｈｉｓｈｉｎｇ Ｒｅｓｉｓｔａｎｔ ＭＦＡ」ガイダンスによると、フィッシング耐性のある認証方法は、「ＦＩＤＯ」か「公開鍵基盤による多要素認証（ＭＦＡ）」であり、多要素認証は実施しないよりは良いが無条件に安全であるわけではなく、ＳＭＳやＩＶＲ（自動音声応答）を用いた認証は最後の手段で一時的な解決にしか繋がらないと評価されている。国内の状況としては、特に、令和５年度はフィッシングによるものとみられるインターネットバンキングの不正送金被害が急増して

おり、決済サービスにおいてフィッシング耐性のある多要素認証方式を導入することは重要であると考える。単に認証の数を増やすだけでは、認証強度が高まらず、ユーザーの手間のみを増やす結果となりうるため、不正利用の手口に対して効果的な多要素認証を考えることが重要である。なお、当人認証の強化では、ユーザーが詐欺等で騙されて自ら操作してしまう場合は防ぐことができない。そのため、ユーザーが異変に気付く工夫や継続的な注意喚起を行う等の対応も不可欠である。

次に、当行のフィッシング対策について、①インターネットバンキングまたはアプリの送金、②他社決済サービスへの即時口座振替によるチャージ、の取組を説明する。

①インターネットバンキングまたはアプリの送金では、ゆうちょ認証アプリによるＦＩＤＯ認証、もしくはハードウェアトークンによるトランザクション認証を行うことで、振込手続きが完了となる。 当行の特色として、ゆうちょ認証アプリの利用登録時に、口座番号／暗証番号等とＳＭＳ／ＩＶＲによるワンタイムパスワードに加えて、ｅＫＹＣのへ方式（本人確認書類のＩＣチップ読取等）による確認を行うことでゆうちょ認証アプリに登録できるようにしている点がある。ただし、ｅＫＹＣのへ方式による認証を必須とすると、利用できないお客さまが出てくるため、選択制としている。認証を行ったお客さまは、即時で利用開始可能で、かつ取引に制限も設けない。一方、認証を行わなかったお客さまは申込から 24 時間後より利用可能となるリードタイムを設け、１日あたりの送金限度額を５万円に引下げて設定する等、取引を一部制限している。

被害を発生させないためにはサービスの入口で防ぐことが重要で、当行ではお客さまの資産を守るためにも認証アプリの登録時にｅＫＹＣを求めており、最近では、ｅＫＹＣ手続きが各社のサービスで利用されているためか、お客さまのｅＫＹＣに対する拒否感も薄らいできている印象がある。なお、認証アプリ登録後は、利便性とセキュリティが両立できるＦＩＤＯ認証で送金ができるため、お客さまの利便性も満たせると考えている。

②他社決済サービスへの即時口座振替によるチャージは、決済サービスと預金口座の紐づけ時に認証を行い、紐づけ後のチャージ、決済等では連携元の銀行で取引の都度認証を行わず、連携先の決済サービス上で認証操作を行えばチャージ等できる仕組みが一般的である。ＣＢＤＣにおいても同様のフローを想定するのであれば、預金口座とＣＢＤＣ口座の紐付け時の認証は重要になると考える。当行では、決済サービスと預金口座の紐付け時に考えられるリスクに対して主に２点の対策を行っており、①銀行口座紐づけ時に連携さ

れる銀行側の身元確認済情報を基にしたアカウント開設（犯罪収益移転防止法 13 条の特例：銀行依拠）は不可とし、連携先アカウント情報と預金口座情報の一致確認を連携先に求めること、②預金口座紐づけ時にはワンタイムパスワードを用いて口座情報を連携することが挙げられる。これらの対策を組み合わせることで当行を狙ったリアルタイムフィッシングのリスクを低減している。ただし、現在被害が起きていないとしても、どのような被害が発生しうるかを想定して、その対処方法を事前に検討しておくことは、サービス提供者側として不可欠である。

当人認証におけるＣＢＤＣの検討課題に関して、これまでの会合でも挙げられたが、ガイドラインについて言及したい。

新規サービスの開始時はセキュリティに穴が生じやすく悪意者から狙われやすい。仮に、サービス開始当初に問題が起きるとサービス自体の印象が悪くなり、過去にはサービス廃止に至った事例もあったと認識している。そのため、デジタル庁やＯｐｅｎＩＤファウンデーション・ジャパンのガイドライン等を参考に、ＣＢＤＣにおいてもガイドラインを策定し、最新の脅威動向を反映し、速やかに改定していく必要があるのではないだろうか。その際に、ガイドラインの本質的な理解を促すために陥りやすい実装不備事例等が共有されることも有意義であろう。ＣＢＤＣは全国民が利用対象となるのであれば、潜在的な被害も大きくなる可能性があるために、セキュリティを重視する立場からは、利便性よりも安全性を重視することが望ましいと考える。

最後に、ＮＩＳＴ等のガイドラインにおいて、当人認証プロセスの厳密さ、強度を示す当人認証保証レベルが３段階で定義されており、そのうち多要素認証を必須とする保証レベル２ではフィッシング耐性のある認証を備えることは推奨の位置づけであるが、将来的にはフィッシング耐性のある認証が必須になるのではないかと考えている。認証のセキュリティとユーザビリティはトレードオフと言われるが、現在ではＦＩＤＯ認証のようにフィッシング耐性を持ちセキュリティとユーザビリティが両立した仕組みが登場している。

３．ディスカッション

プレゼンテーションに引き続き、参加者によるディスカッションが行われた。モデレータは、株式会社ＮＴＴドコモが担当した。概要は以下のとおり。

【新たな当人認証手法の普及とサポート】

（参加者）一般的に、新たな当人認証の方式を、ユーザーへ普及させることは簡単ではないと認識している。普及に向けた苦労や取り組みがあれば教えてほしい。

（参加者）普及に向けては、やはりユーザーに対して継続的にご案内をしていくことに尽きるだろう。

（参加者）サービスの使われ方に応じて、サポートも連動して対応していくことを踏まえると、仮にＣＢＤＣを誰一人置いていかないサービスと位置づけるとすれば、それを達成するためにどのようなサポートが必要となるかを考えていくことは必要だろう。

【リスクに応じた当人認証強度】

（参加者）海外では取引金額の基準を設けて、少額の場合は当人認証強度を緩く設定するという発想があるが、フィッシング被害が日本では過去最大となっている状況を踏まえつつ、どのような対応が望ましいだろうか。

（参加者）各社はフィッシング対策に注力しているが、大量のログを監視の上、不正取引を見つけ出して取引停止等の対応を行うことは容易ではない。取引金額に関わらず、基本的には強固な当人認証を求めて、監視負荷を減らすことが望ましいのではないだろうか。

【セキュリティとコスト】

（参加者）窓口やコールセンターでの問い合わせ対応、不正取引の監視対応などにはコストがかかり、セキュリティを高めるほどコストが嵩むため悩ましい点と考えている。コストをかけて高度な当人認証やサポート体制を構築することが、総合的にはコスト面含めメリットがあるのだろうか、どのように捉えているか。

（参加者）問い合わせや監視対応だけでなく、例えばＦＩＤＯ認証のためのライセンスコストや、ｅＫＹＣを実施する場合の１件あたりのコストなど、セキュアなサービスを提供しようとすると、一定のコストが生じることは避けられない。セキュリティと利便性だけでなく、コストも考慮にいれることは共通の認識と思われ、自社内でもコスト削減は度々議論になる。ただし、コストを抑えるために当人認証を軽くしようといった議論ではなく、セキュリティ水準を維持しながらどうにかコストを抑える工夫ができ

ないかといった議論が主になっている。

【ユニバーサルアクセス】

（参加者）当人認証を強化した結果、新たな方法に対応が難しいユーザーもでてくると思うが、どのような対応が考えられるだろうか。

（参加者）ユーザーごとの状況に応じた工夫やリスクベースの考え方に基づいて対応していくことが必要になるだろう。

【セキュリティと取引上限金額含めたサービス設計】

（参加者）金額基準に応じて当人認証の強度を変える考え方のご紹介があった。一例として、ことら送金は１回の取引上限金額が 10 万円と定められており、少額送金の場合の当人認証を考えるうえで参考になるだろう。既存のインターネットバンキングにことら送金機能を組み込む場合、インターネットバンキングにログイン後、ことら送金利用のためにもう一度当人認証を求める必要はあるか、求めるのであれば通常の振込と同様の認証強度でよいのか等、セキュリティと利便性のバランスを踏まえて検討していく必要があると考える。

（参加者）インターネットバンキングにおいて既存の銀行振込機能に加えて、少額送金に限ったサービスを追加した場合を想定すると、同じセキュリティ水準であれば取引上限金額のない既存の振込機能が悪意者に狙われるのは当然で、少額送金に限ったサービスをわざわざ狙うことはないだろう。とはいえ、銀行振込と少額送金に限ったサービスはセキュリティ水準を同じにする必要があるわけではなく、取引上限金額に応じてセキュリティ水準を異なる設定にすることも有り得ると考える。なぜなら、悪意者が不正対象として狙うインセンティブは、不正行為によって得られる犯罪収益から必要なコストを差し引いた利益がどの程度かによるため、取引上限金額が低ければ、悪意者が得られる利益も少額になり、狙うインセンティブが低くなるためである。ただし、例えば悪意者側の技術革新によって簡単かつ低コストで当人認証を突破できるようになれば、取引上限金額が少額でも狙われる可能性が生まれてくる。このように状況の変化によっては、これまで狙われなかったサービスが狙われる可能性もあり、取引上限金額と悪意者のインセンティブの関係性は変わりうるものとして留意する必要がある。

また、フィッシングの攻撃方法は変遷してきているが、足許ではＳＮ

Ｓを用いた投資・ロマンス詐欺が増え、セキュリティの突破よりも直接的に本人をだます手口にシフトしている可能性もある。そうすると、根本的な問題は、ユーザー自身の投資やセキュリティに対するリテラシーの低さとなる。ＣＢＤＣをどのように位置づけるか次第であるが、極端な例を出すと、誰もが使えるユニバーサルサービスとする場合、コストはかかってもセキュリティ水準を上げ、悪意者のインセンティブが働かない程度に取引上限金額を低く抑える設計が考えられるか。他方、リテラシーの高い人しか使えないライセンス制のサービスであれば、取引上限金額を高く設定してもセキュリティ水準は最低限でもよい、自己責任を基本とする設計も考えられる。

ＣＢＤＣを検討する上では、こうしたことを踏まえて、取引上限金額含めどのようなサービス設計とするかが重要なポイントになるだろう。

（参加者）ライセンス制のサービスは難しいだろうが、近い考えとして、使い始める申込時に手続きの内容理解や意思確認をしっかりと求める形にし、利用時は利便性を優先する方法もある。

（参加者）取引上限金額は、ユーザー数によっても考え方は異なると考えている。ユーザー数が多ければ、１万円を１万人から騙し取るやり方が出てきて、総額では多額になる可能性もあるだろう。必ずしも金額の多寡だけではなく、こうしたユースケースやユーザー規模も踏まえて取引上限金額を検討していく必要があるだろう。

【当人認証におけるガイドラインや技術仕様】

（参加者）これまでの会合では、ＣＢＤＣに関して何らかのガイドラインのような仕組みがあった方がよいだろうという意見が出ており、当人認証に関しても同様ではないかと思うが、いかがか。仮に、あった方がよい場合は、どのように決めていくか等のご意見あるか。

（参加者）例えばフィッシング対策であれば民間企業が集まったフィッシング対策協議会、資金移動業者のサービスと銀行口座紐付けであれば金融庁、全国銀行協会などの公的機関や公的機関に近い団体がガイドラインを策定している事例がある。ＣＢＤＣに置き換えて考えると、ＣＢＤＣの協会等、何らかの団体を設立して、その団体がガイドライン作成を担うという議論もありうるだろう。

（参加者）ＣＢＤＣの中央システムを運営するであろう日本銀行が、ガイドライン作成を担うのが良いのではないだろうか。また、各仲介機関がＣＢＤＣの中央システムにアクセスする際に要求される技術仕様として定めてしまえば、そもそもガイドラインである必要もない。必ずしも日本銀行が独力で作るということではなく、フィッシング対策協議会や日本サイバー犯罪対策センター等のノウハウのある協会や団体の意見を聞きながら、技術仕様を定め、定期的に見直していくのが良いだろう。なお、全銀協含めて民間団体が作成したガイドラインでは強制力はないが、技術仕様とすれば必ず対応せざるを得ないので、こうした面でも曖昧にならず良いのではないか。

（日本銀行）海外、特に欧州ではガイドラインを作成するといった議論がなされているところもあるが、日本国内はそのような検討状況には至っていない。ガイドライン等については、その要否含めて、何も決まっていない段階ではあるが、今後も皆様からご意見を頂戴したいと思っている。

（参加者）過去事例から考えると、料金収納を行う官公庁、地方公共団体、企業、金融機関等の事業者が銀行サービスを便利に使うという観点において、日本マルチペイメントネットワーク推進協議会が実質的に事業者と銀行を繋ぐ機能を果たしていた印象がある。もしかしたら、こうした座組はＣＢＤＣにおいても参考になるかもしれない。

（参加者）ガイドラインよりも、技術仕様として定めることに賛同する。過去の事例だが、銀行ＡＰＩのオープン化においてガイドラインが出されたものの、各銀行、各ベンダーが切磋琢磨した結果、それぞれ仕様の異なるＡＰＩの提供に繋がってしまったと感じている。こうした経験も踏まえ、ガイドラインよりも、技術仕様を定めて公開し、どの事業者であっても同じ技術仕様で参入するほうが良いのではないだろうか。

４．次回予定

次回の会合は４月 16 日（火）に開催予定。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第６回会合参加者

（参加者）※五十音・アルファベット順
株式会社イオン銀行
セコム株式会社
ソニー株式会社
大日本印刷株式会社
株式会社千葉銀行
日本電気株式会社
日本マイクロソフト株式会社
日立チャネルソリューションズ株式会社
フェリカネットワークス株式会社
株式会社ふくおかフィナンシャルグループ
株式会社マネーフォワード
株式会社みずほ銀行
株式会社三井住友銀行
株式会社三菱ＵＦＪ銀行
株式会社ゆうちょ銀行
株式会社りそなホールディングス
ＮＲＩセキュアテクノロジーズ株式会社
株式会社ＮＴＴドコモ
ＰａｙＰａｙ株式会社

（事務局）
日本銀行

別添1
セコム株式会社

CBDCフォーラム WG3
第6回会合
当人認証の現状および最新動向の整理

2024年3月25日

セコム株式会社 IS研究所
デジタルプラットフォームディビジョン
主幹研究員
佐藤　雅史

この発表では…

今後の当人認証の議論で必要と思われる

- 当人認証をとりまく全体的な俯瞰と、概念や言葉の整理
- 当人認証の議論でよく出てくる最近の話題の言葉
  Identity Wallet, Verifiable Credentials

を議論し、

- CBDCに関わる当人認証の論点を提示する

ことを目標としたいと思います。

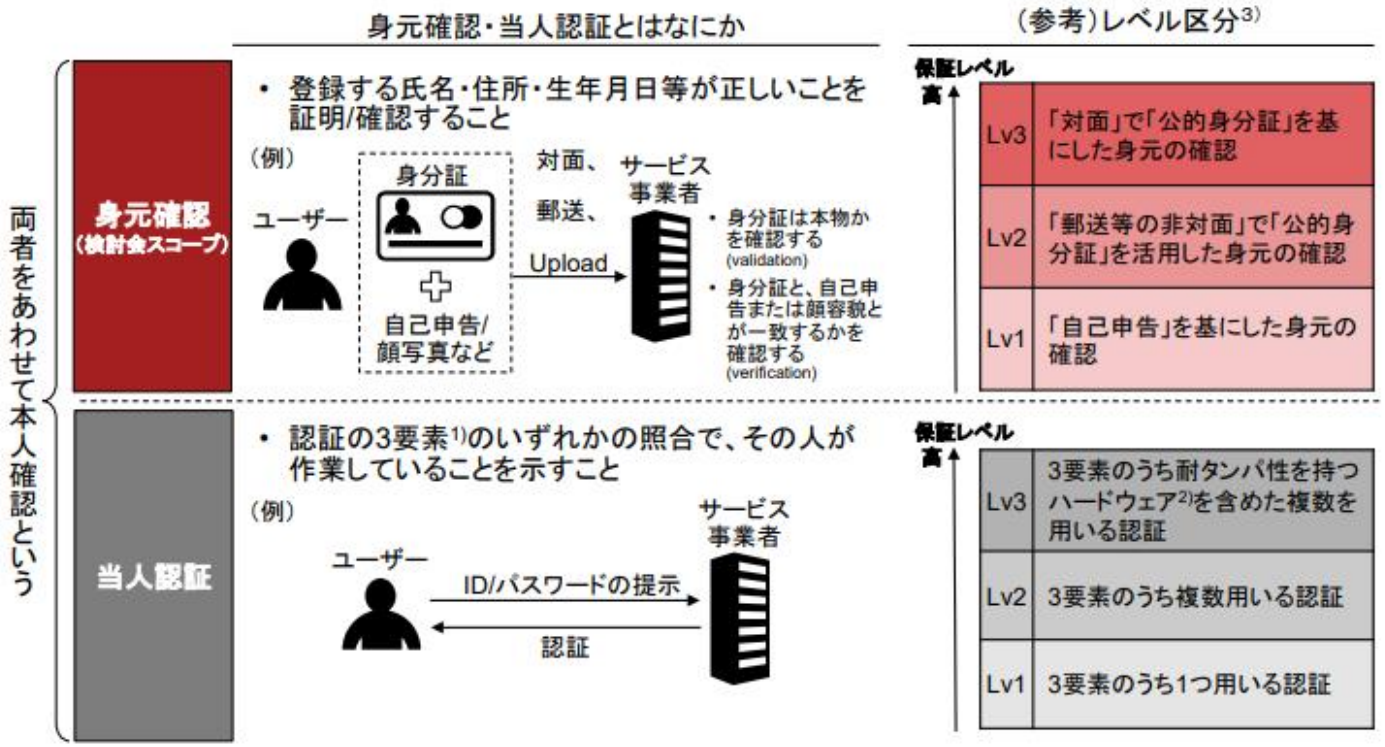
本人確認？身元確認？当人認証？

セコムIS研究所
Intelligent Systems Laboratory

オンラインサービスにおける身元確認手法の整理に関する検討報告書（概要版）
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf

1.「身元確認」の「当人認証」との区別

「身元確認」は、ユーザー当人の実在性を確認し、「当人認証」は、ユーザーの行為を確認する。通常両方の組み合わせを通じて「本人確認」が行われている。



1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）のレベル区分

経済産業省 NEDO Strategy&

ここから先の話（特に用語や概念）はNIST SP800-63 A,Bを参考にしています。

身元確認～当人認証に至る全体のイメージ

セコムIS研究所
Intelligent Systems Laboratory

申込時(再登録時)

①取引時確認 （CDD）
- 身元確認（Identity Proofing）
- 顧客管理事項の確認
- その他確認事項の確認

※サービスのリスクに応じて身元確認を実施

②登録（Enrollment）
- サービスアカウントの作成
- 認証器/認証手段（Authenticator）の発行
- 認証器のバインディング
- （連携IDの登録）

サービス利用時

③当人認証（Authentication）
- 認証器がユーザーの管理下にあることの確認
- ユーザー識別子・認証器による出力結果の検証

④サービス機能の利用
- オンラインサービスが提供する機能の利用
- API利用の認可

身元確認と登録

セコム IS研究所
Intelligent Systems Laboratory

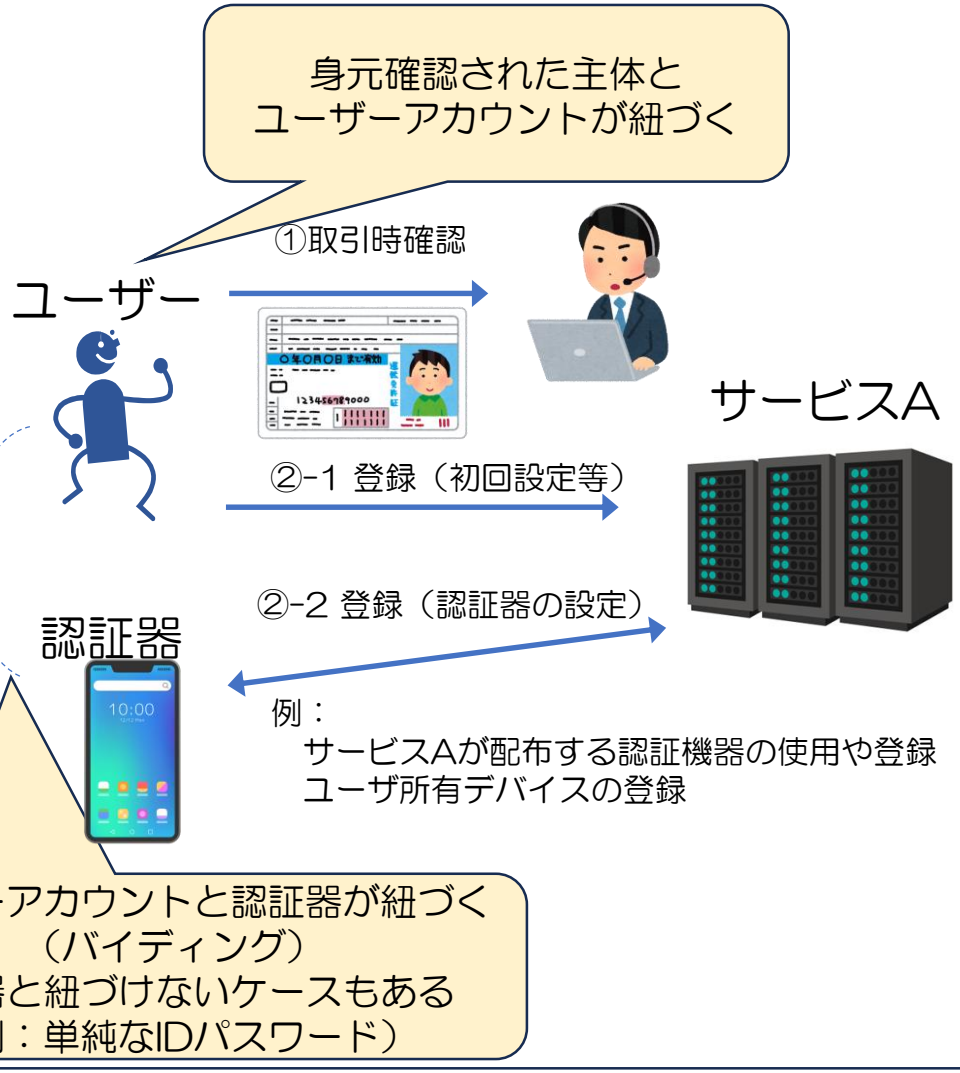
申込時(再登録時)

①取引時確認 （CDD）
- 身元確認
- 顧客管理事項の確認
- その他確認事項の確認

※サービスのリスクに応じて身元確認を実施

②登録（Enrollment）
- サービスアカウントの作成
- 認証器（Authenticator）の発行
- 認証器のバインディング
- （連携IDの登録）

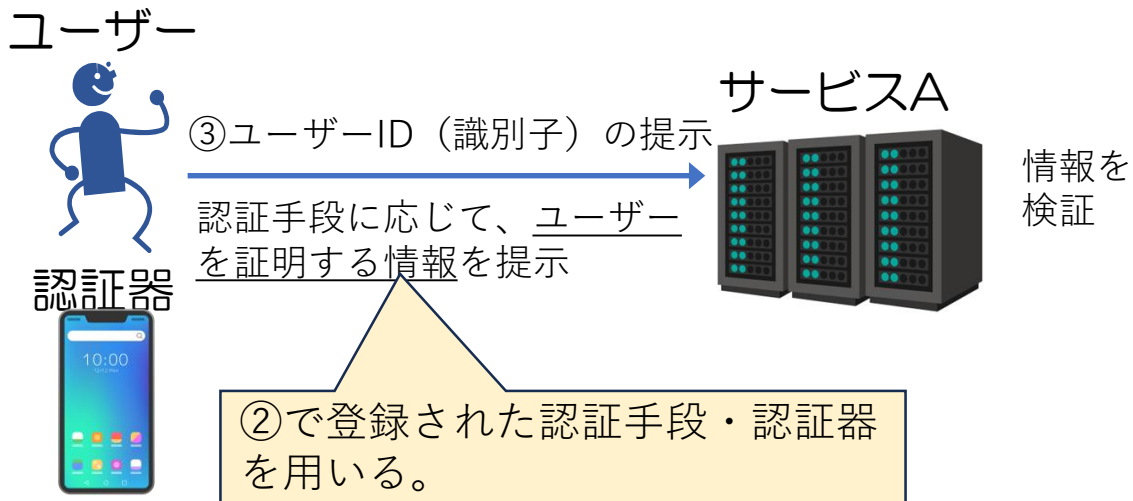
申込時のフローのイメージ



当人認証

セコム IS研究所
Intelligent Systems Laboratory

当人認証のイメージ



サービス利用時

③当人認証（Authentication）
- 認証器がユーザーの管理下にあることの確認
- ユーザー識別子・認証器による出力結果の検証

④サービス機能の利用
- オンラインサービスが提供する機能の利用

ID連携

セコムIS研究所
Intelligent Systems Laboratory

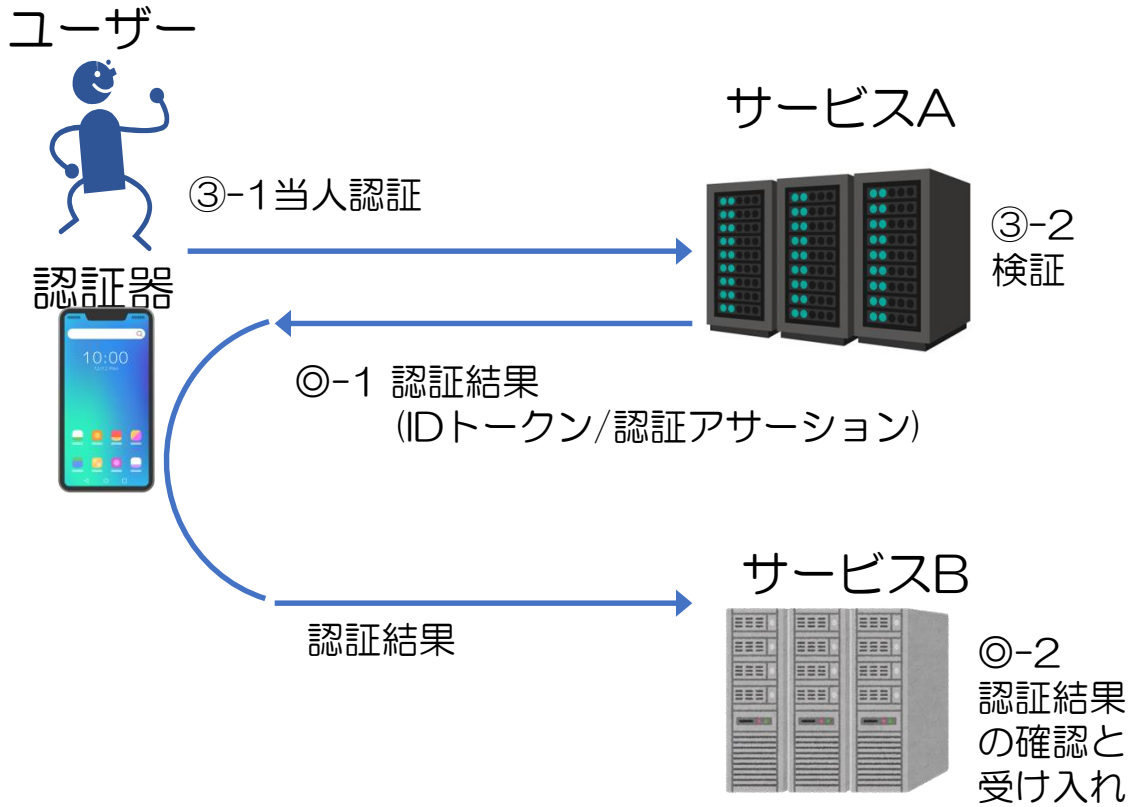
サービス利用時

③当人認証（Authentication）
- 認証器がユーザーの管理下にあることの確認
- ユーザー識別子・認証器による出力結果の検証

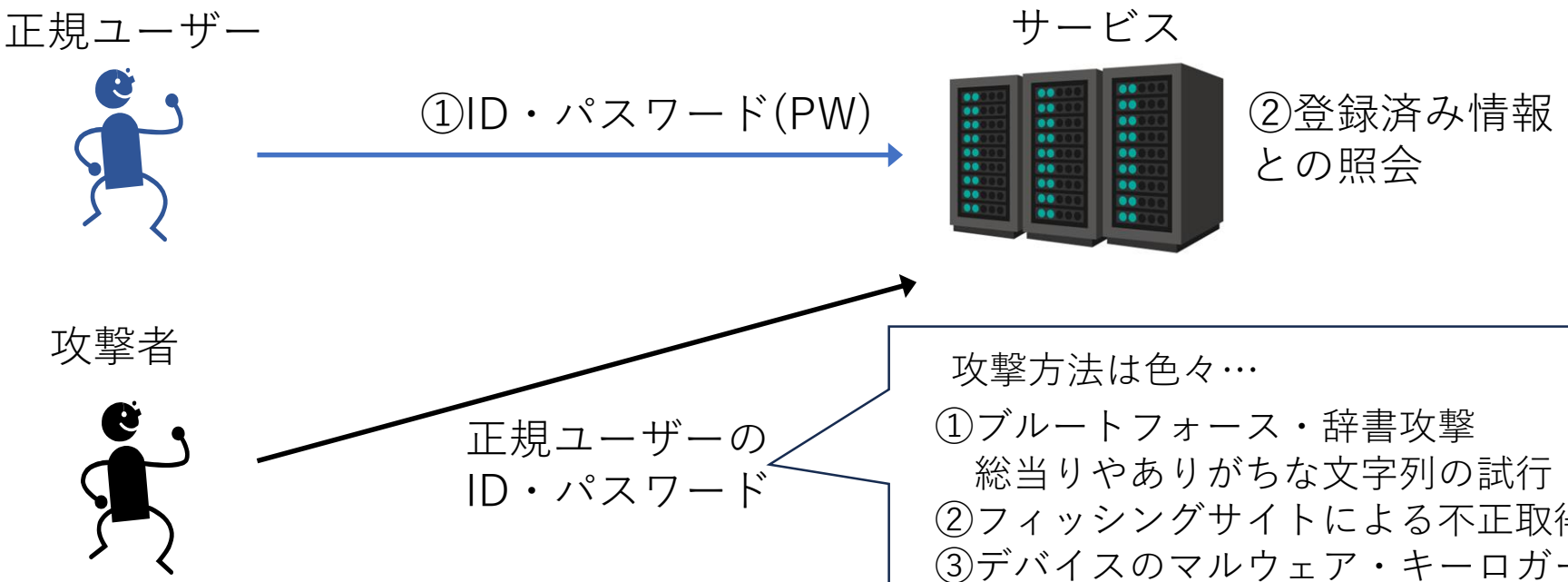
◎ID連携（Federation）
- システム間での当人認証結果の伝達と連携

④サービス機能の利用
- オンラインサービスが提供する機能の利用

ID連携のイメージ



当人認証手段(単純なID/PW)の不正利用



当人認証の認証手段・認証器の種類

セコムIS研究所
Intelligent Systems Laboratory

- **知識：Something you know**
  例）パスワード
  下記の「所持」におけるハードウェアトークンやデバイスを活性化するためにも使用される。
- **所持：Something you have**
  例）ワンタイムパスワード（OTP）デバイストークン、暗号鍵（署名鍵）を格納するハードウェアトークン、デバイスにインストールしたソフトウェア（OTP, 暗号ソフトウェア）※電子メールは該当しない
- **（生体認証：Something you are）**
  例）指紋、音声など。
  上記の「所持」と組み合わせて、ハードウェアトークンやデバイスを活性化する際に使用する。特定条件下でオンラインで生体認証を行うケースもありえる。

認証器の形態や実装により、特性がある。
認証器により対策可能（軽減可能）な脅威や、認証器自身への脅威も異なる。
多要素認証では「知識」＋「所持」や「生体認証」＋「所持」の組み合わせで使用される。
⇒　**本セッション後半（ゆうちょ銀行様）で議論**

当人認証における脅威 ※具体的な脅威は実現方法に依存する

セコムIS研究所 Intelligent Systems Laboratory

登録時

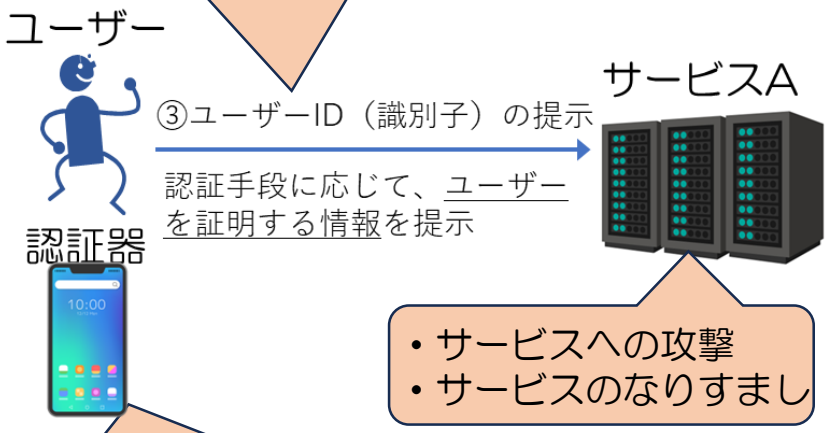
身元確認書類の不正や
人物偽装によるなりすまし

登録プロセスの不具合や不正利用
による不正な認証器への紐づけ

※再登録時（紛失・盗難等）に要注意

当人認証

認証プロトコルへの攻撃・不正利用
（例：改ざん、再送攻撃、盗聴、中継）

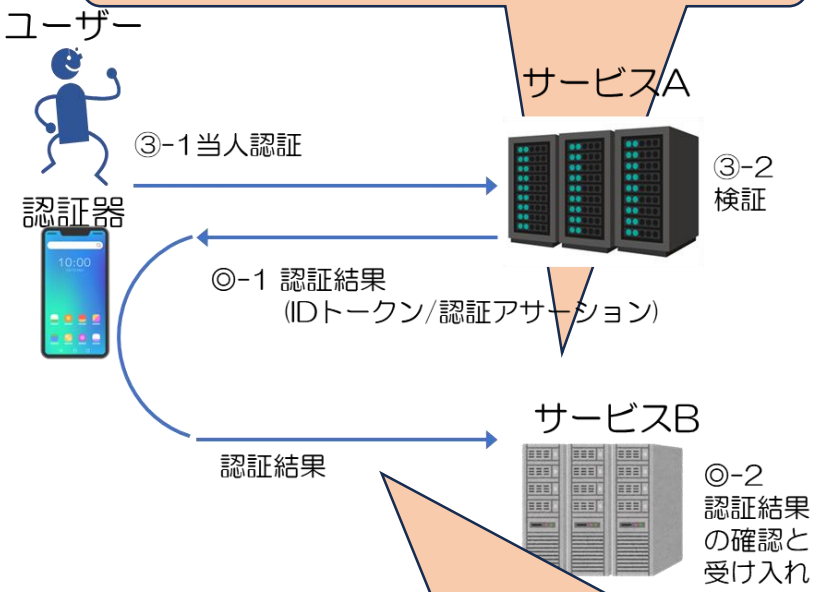


・サービスへの攻撃
・サービスのなりすまし

認証器への攻撃・不正利用

連携時

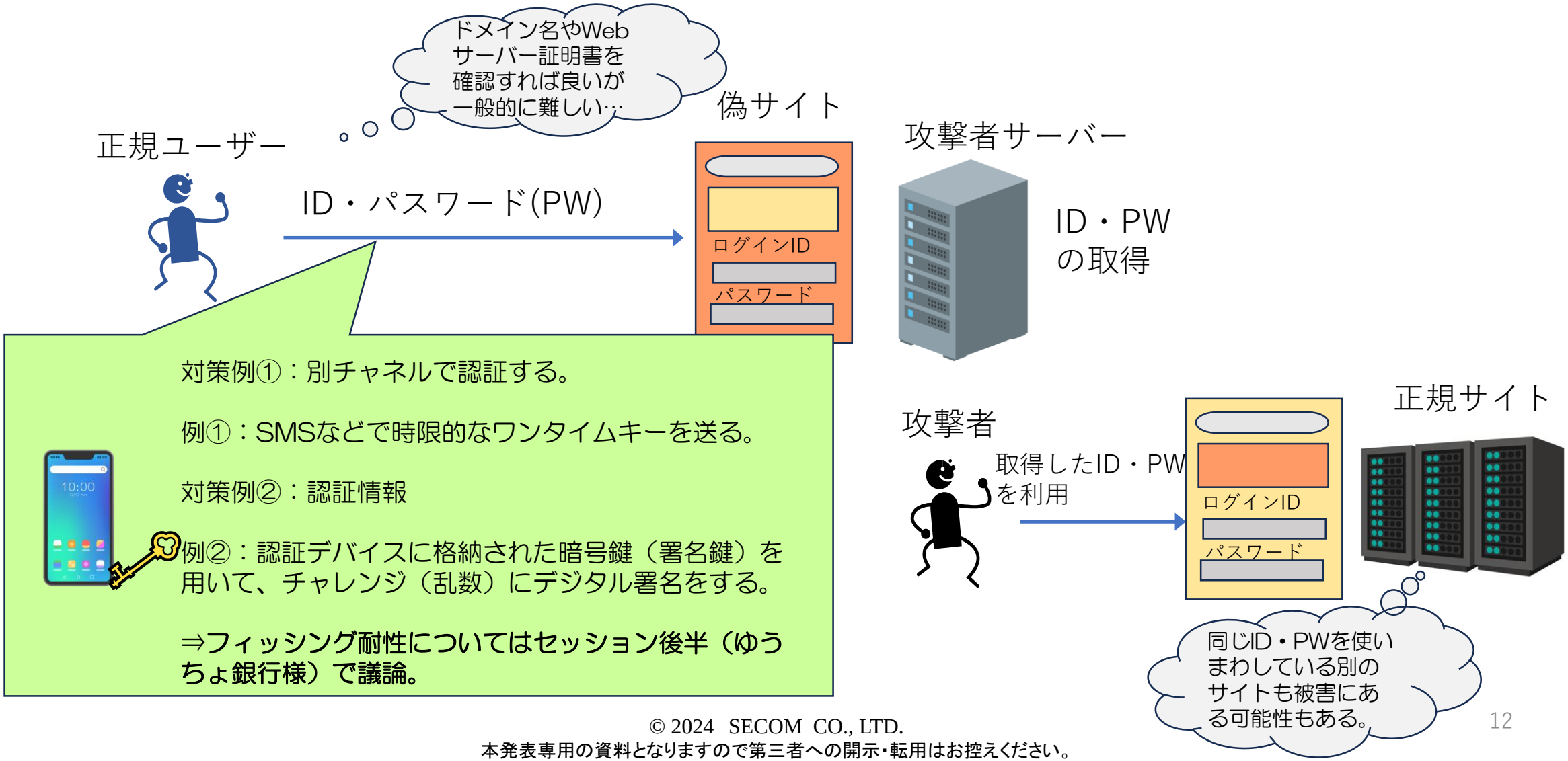
連携サービスの身元確認・当人認証レベルの相違による不適切な利用



認証結果（IDトークン,アサーション）
の不正利用

その他
- サービス機能やAPIの不具合や不正利用による上記の工程を迂回した不正アクセス
- APIの認可プロセスの不具合や不正利用による不正アクセス

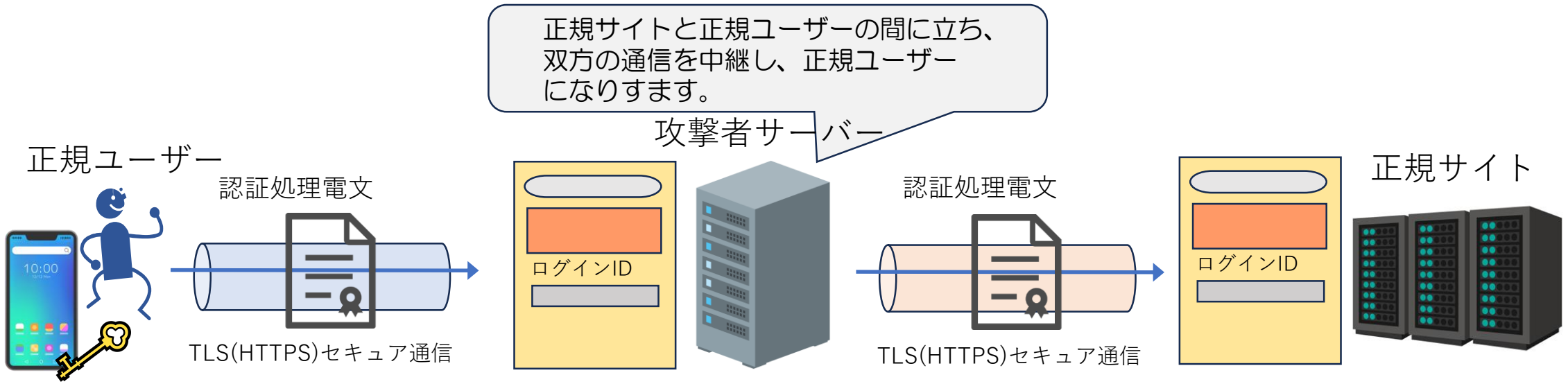
当人認証における脅威の例①
フィッシング（認証情報の不正な収集）



当人認証における脅威の例②
中間者攻撃（リアルタイムフィッシング）

単純にワンタイムパスワードやデジタル署名にするだけでは防げないケース。

正規サイトと正規ユーザーの間に立ち、
双方の通信を中継し、正規ユーザー
になりすます。



認証処理電文だけを見ると
正規サイトと通信しているように見える。

認証処理電文だけを見ると
正規ユーザーからのものに見える。
実際には攻撃者サーバーがアクセスしている。

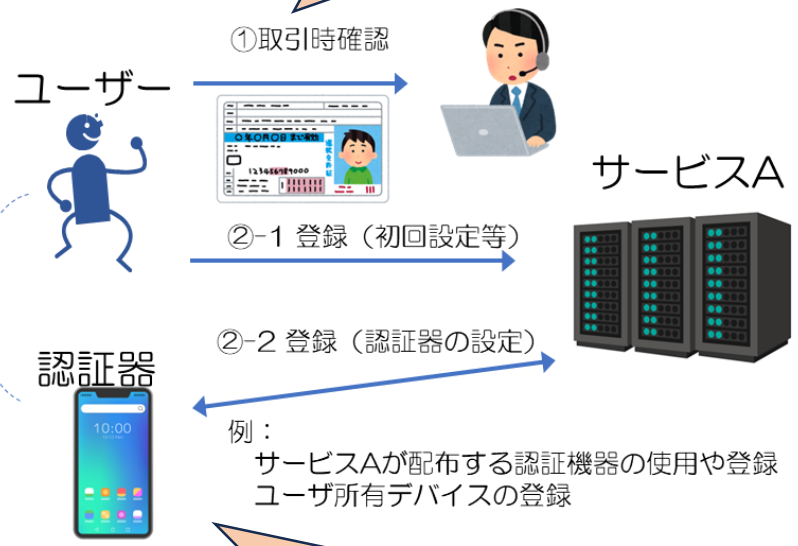
対策の基本的な考え方として、認証処理電文が意図した通信相手からのものであることを
互いに確認することが必要。
例：登録済みドメインに限定した送信、セキュア通信（TLS）と認証処理電文の紐づけ、
　　ユーザークライアントとサーバー間による認証処理電文送信元の確認（オリジンの確認）
　　⇒抜本的な対策として認証プロトコルでの対応が必要（WebAuthn規格等）

当人認証における脅威 ※具体的な脅威は実現方法に依存する

セコムIS研究所 Intelligent Systems Laboratory

登録時

身元確認書類の不正や
人物偽装によるなりすまし



登録プロセスの不具合や不正利用
による不正な認証器への紐づけ

※再登録時（紛失・盗難等）に要注意

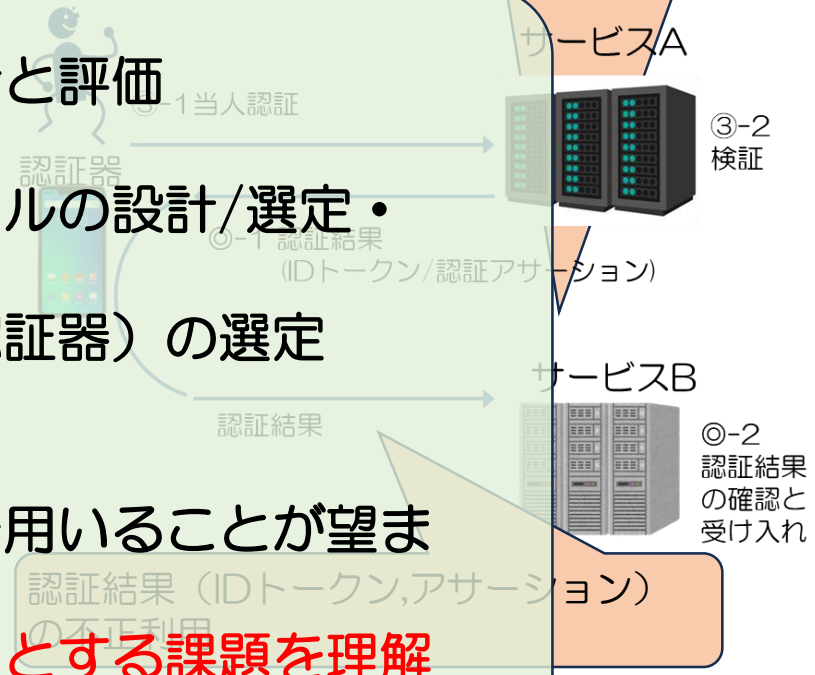
当人認証

認証プロトコルへの攻撃・不正利用
（例：改ざん、再送攻撃、盗聴、中継）

認証器への攻撃・不正利用

連携時

連携サービスの身元確認・当人認証レベルの相違による不適切な利用



- サービスへの攻撃
- サービスのなりすまし

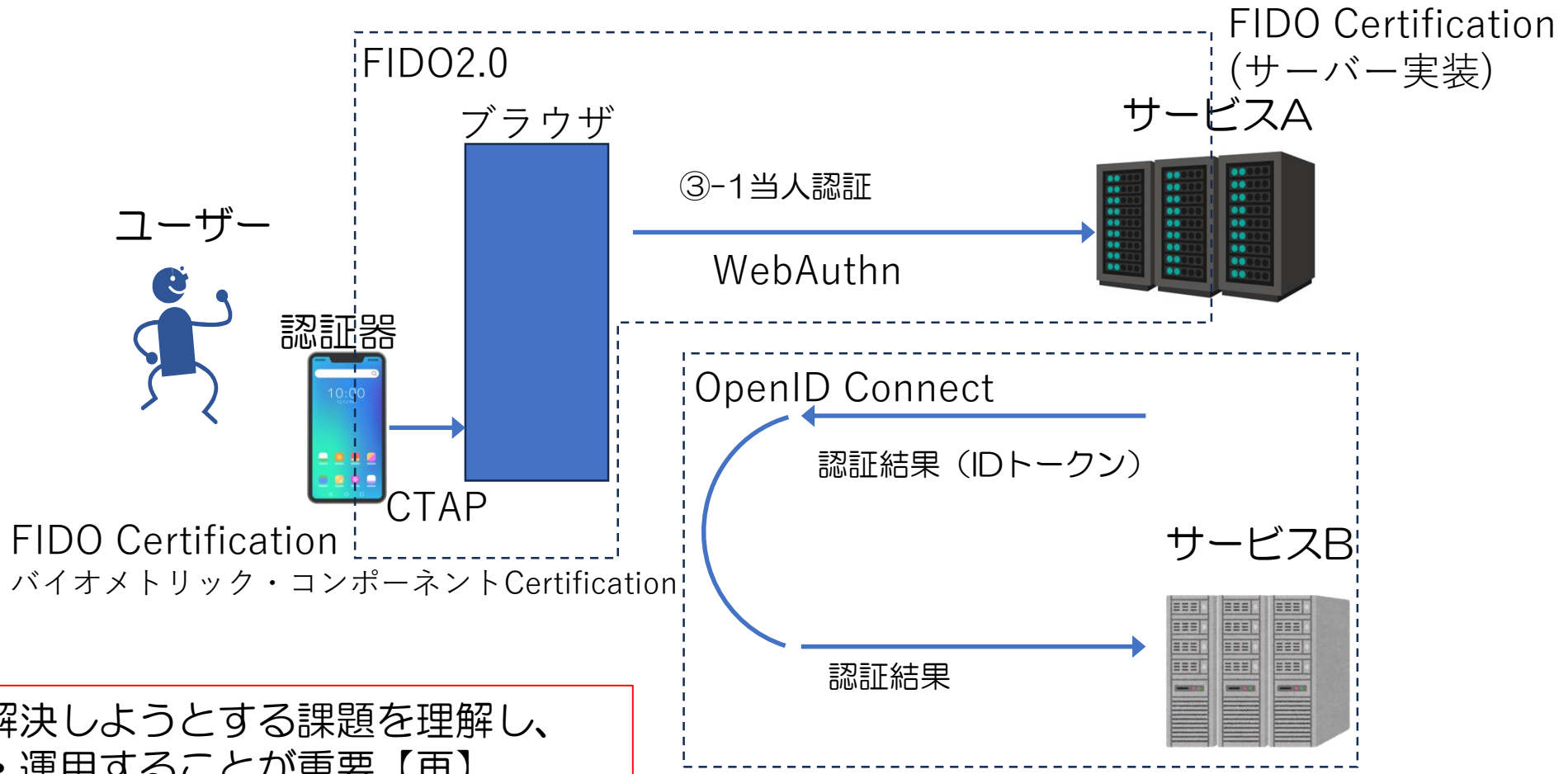
その他
- サービス機能やAPIの不具合や不正利用による上記の工程を迂回した不正アクセス
- APIの認可プロセスの不具合や不正利用による不正アクセス

①脅威とリスクの分析と評価
② ①に基づいた
- 適切な認証プロトコルの設計/選定・実装
- 適切な認証手段（認証器）の選定

可能な限り標準規格を用いることが望ましい。
標準規格が解決しようとする課題を理解し、適切に実装・運用することが重要。

当人認証に関する標準規格の例

～FIDO, OpenID Connectの一例～



標準規格が解決しようとする課題を理解し、
適切に実装・運用することが重要【再】

当人認証に関するガイドラインの例

～NIST SP 800-63 Digital Identity Guidelines～

セコムIS研究所 Intelligent Systems Laboratory

身元確認や当人認証に関わるガイドライン。米国政府機関や民間企業で参照されているガイドライン。
63A（登録と身元確認）、63B（当人認証）、63C（連携）にて各要件を規定。
2023年には最新のRevision 4の改定（案）が公開された。

SP800-63-3Bが定める認証器の分類

AAL	レベル1	レベル2		レベル3
概要（一部）	ユーザーが認証器を制御していることの**ある程度の保証**。 単一または多要素の認証器。	ユーザーが認証器を制御していることの**高い確実性**。 単一の多要素認証器または２つの単一要素認証器。		ユーザーが認証器を制御していることの**極めて高い確実性**。 暗号鍵の所有を証明する認証器。
選択可能な認証器の種類	以下のいずれか。 • 記憶シークレット • ルックアップシークレット • アウトオブバンドデバイス • 単一要素ワンタイムパスワード(OTP) デバイス • 多要素 OTP デバイス • 単一要素暗号ソフトウェア • 単一要素暗号デバイス • 多要素暗号ソフトウェア • 多要素暗号デバイス	どちらか	以下のいずれかの多要素認証器 • 多要素 OTP デバイス • 多要素暗号ソフトウェア • 多要素暗号デバイス ※Rev4案では多要素アウトオブバンド認証器も	以下のいずれか • 多要素暗号デバイス • 単一要素暗号デバイスを記憶シークレットと併用 • 多要素 OTP デバイス(ソフトウェアまたはハードウェア) を単一要素暗号デバイス と併用 • 多要素 OTP デバイス(ハードウェア)を単一要素暗号ソフトウェアと併用 • 単一要素 OTP デバイス(ハードウェア) を多要素暗号ソフトウェアと併用 • 単一要素 OTP デバイス(ハードウェア) を単一要素暗号ソフトウェア及び記憶シークレットの併用 ※フィッシング耐性/中間者攻撃耐性も必要 ※Rev4案では最後の候補を削除
			記憶シークレットと以下のいずれかの認証器（所持ベース） • ルックアップシークレット • アウトオブバンドデバイス • 単一要素 OTP デバイス • 単一要素暗号ソフトウェア • 単一要素暗号デバイス	

当人認証における脅威 ※具体的な脅威は実現方法に依存する

セコムIS研究所 Intelligent Systems Laboratory

登録時

身元確認書類の不正や人物偽装によるなりすまし

標準規格では詳細がカバーされない範囲で、運用を含めた対応が必要。
サービス提供事業者に応じて、登録時のフローの設計や運用が行われる。
（ここがとても大切）

登録時のバインディングは要注意。例えば、再登録時のプロセスが簡易な場合ではリスクがある。
⇒本セッション後半（ゆうちょ銀行様）で議論

当人認証

認証プロトコルへの攻撃・不正利用
（例：改ざん、再送攻撃、盗聴、中継）

ユーザー

認証器

認証器への攻撃・不正利用

連携時

連携サービスの身元確認・当人認証レベルの相違による不適切な利用

サービスA

③-2 検証

◎-2 認証結果の確認と受け入れ

サービスB

認証結果（IDトークン,アサーション）の不正利用

①脅威とリスクの分析と評価
② ①に基づいた
・適切な認証プロトコルの設計/選定・実装
・適切な認証手段（認証器）の選定

可能な限り標準規格を用いることが望ましい。
標準規格が解決しようとする課題を理解し、適切に実装・運用することが重要。

その他
- サービス機能やAPIの不具合や不正利用による上記の工程を迂回した不正アクセス
- APIの認可プロセスの不具合や不正利用による不正アクセス

当人認証に関わる要注意な用語

クレデンシャル（Credential）？

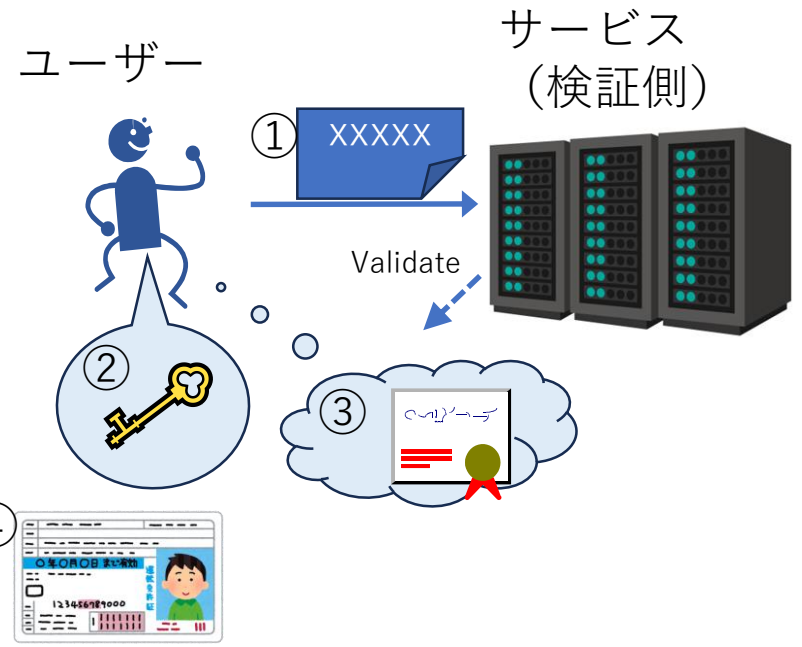
① 当人認証において、ユーザー等の対象が自身の証拠として検証相手に提示するデータを意味するケース
- 例：パスワード、パスワードから生成したデータ

② 当人認証において、ユーザー等の対象が管理する秘密情報を意味するケース
- 例：パスワード、秘密鍵（署名鍵）

③ 当人認証において、ユーザー等の対象に関する情報（検証するためのデータ）を意味するケース
- 例：電子認証局から発行される電子証明書（PKIの公開鍵証明書）
- RFC4949的定義：識別子と当人認証の情報の関係を示したデータ

④ ユーザー等の対象の属性や資格の証明を意味するケース
- 例：IDカード、運転免許証、後述のVerifiable Credentials

など
文脈や標準規格により用語の定義が異なる。
〇〇 Credentialという言い方で区別することもある。



認証？
（和訳が混同するケース）

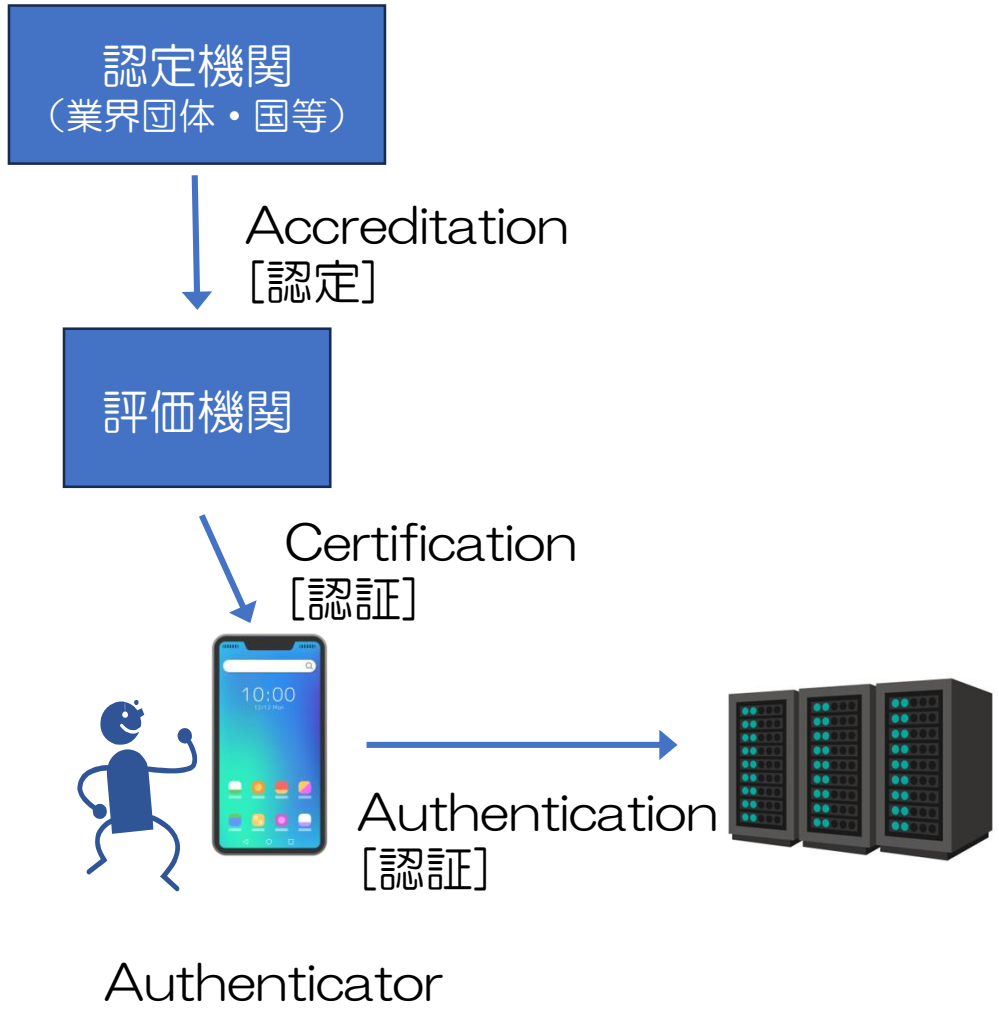
- Authentication [認証]

混同しやすい

- Certification [認証]

混同しやすい

- Accreditation [認定]



検証？
（和訳が混同するケース）

- Verification
  ある値や事実の真偽や正確さを確認する。
- Validation
  健全性や妥当性を確認する。

例：ユーザーが入力したパスワードの一致性が確認できる。

例：デジタル署名済みデータの正しさをユーザーの検証鍵で確認できる。

例：ユーザーの電子証明書が信頼できる認証局から発行されており、有効期限が切れていない、失効されていない。

当人認証のプロセスではVerificationとValidationが複合的に行われることがある。

他にも…

- Attestation
- Assertion
- Claim
- Token

などなど

他の言葉と区別が難しく、日本語にも訳しにくい用語がたくさんあることが悩ましいところです…

セコムIS研究所
Intelligent Systems Laboratory

新たな技術動向

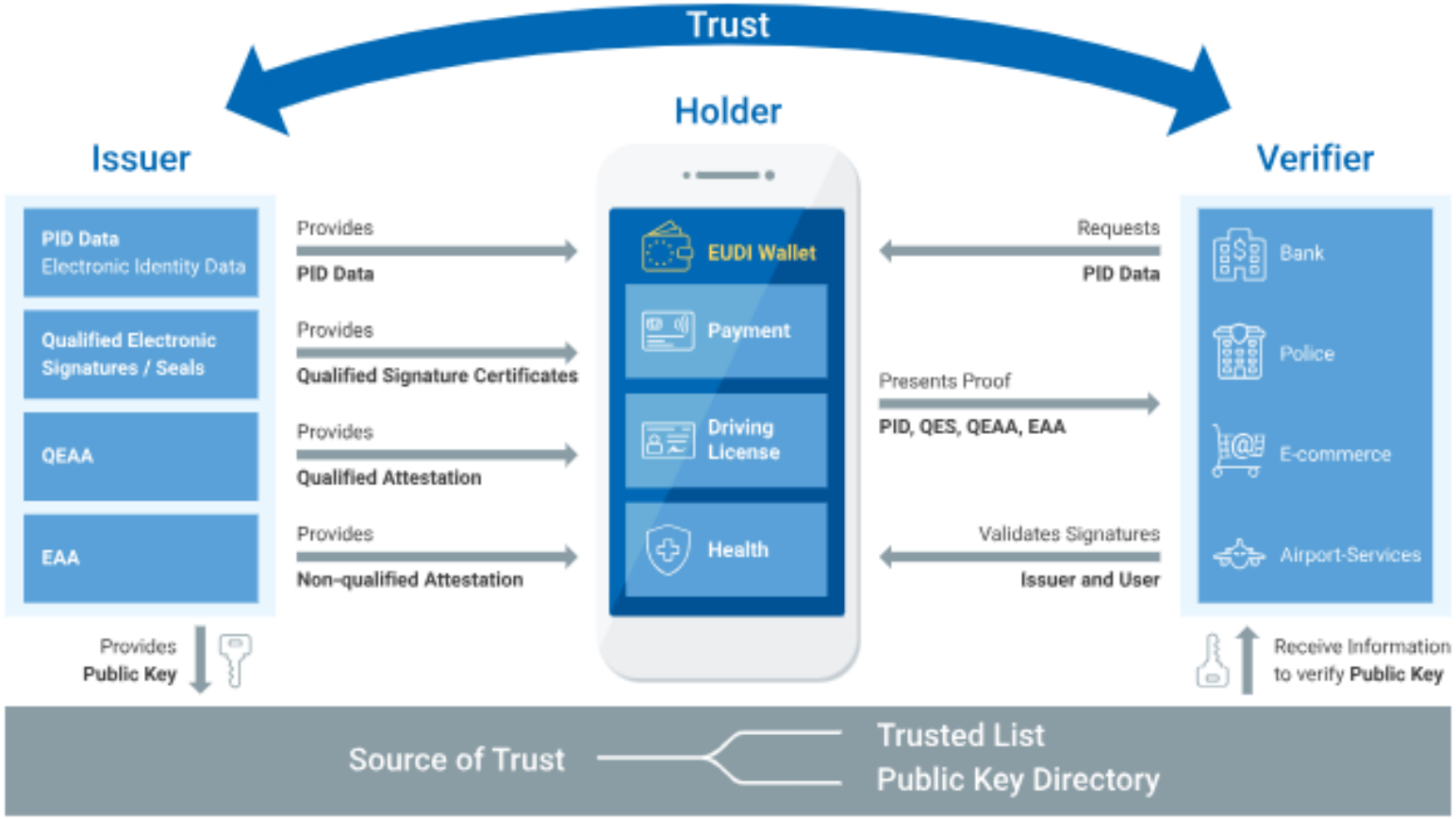
技術動向①

Digital Identity Wallet (EU)

- スマートデバイスに搭載されるウォレット。以下を含んだ機能を提供。
  - ◆デジタル証明書（身分証明や属性証明）の格納
  - ◆当人認証
  - ◆電子署名（否認防止）
- プロトコルや要件を定めた標準仕様の規定。
- 適合性評価と認証の制度(Certification)。

EUで基準を定め、EU加盟国がウォレットの実装を提供する。

日本においても、CBDCも視野に入れたウォレットの標準化に関する考え方について参考になる。

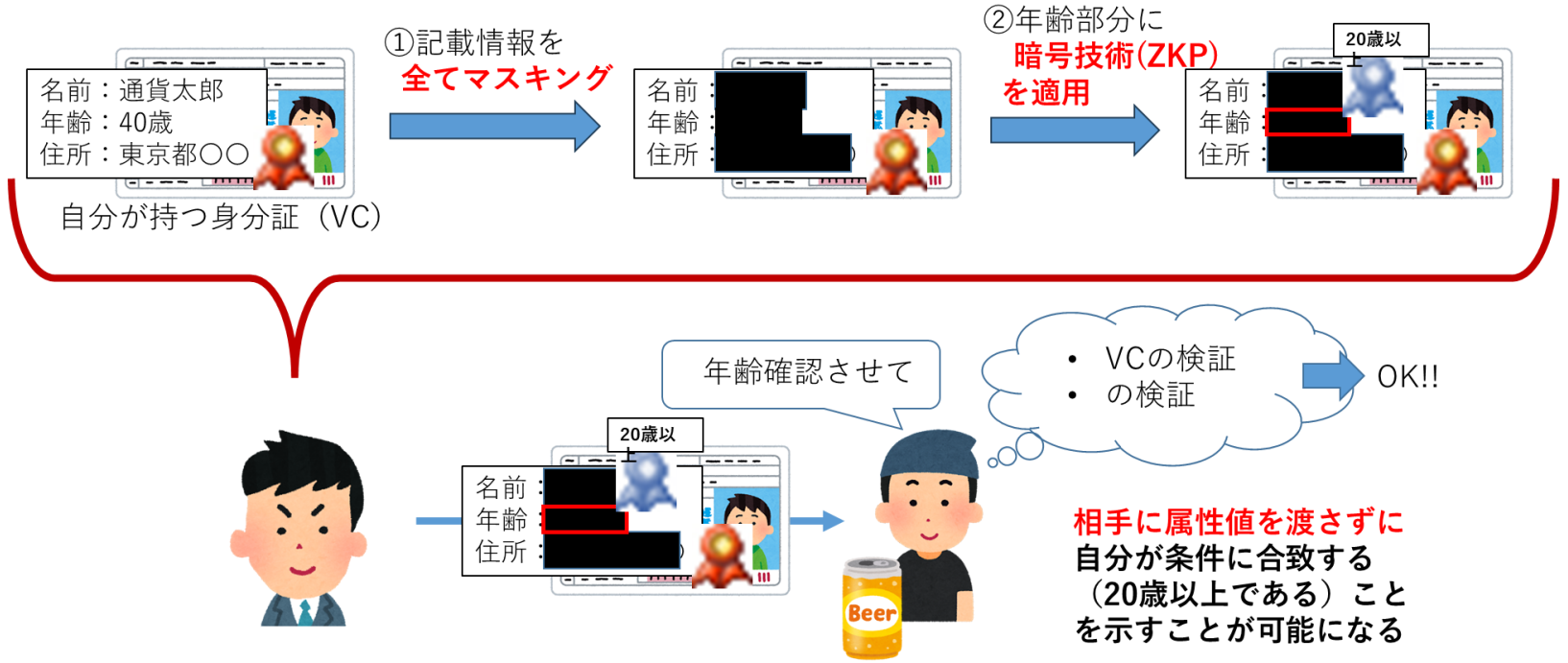


https://utimaco.com/ja/news/blog-posts/eidas-20-roadmap-toolbox-and-european-digital-identity-wallet-architectureより引用

技術動向②
Verifiable Credentials

セコムIS研究所
Intelligent Systems Laboratory

- デジタル版の証明書（身分証明書や属性証明）。
- 自己主権型
  証明書の非改ざん性を維持したまま、ユーザーの意思によって開示できる情報をコントロールできる（選択的開示やゼロ知識証明の適用）。
  IDプロバイダーによる認証連携とは異なるモデルになりえる。
- 標準化
  - ◆ データモデルやフォーマット等についてW3Cで標準化が行われている。
  - ◆ OpenID Foundationでは発行や格納のプロトコルを規定。
  - ◆ EU Digital Identity Walletでも参照されている。



- 考えられる用途の例
  - ◆ デジタル証明書（本人確認書類や資格証明など）による身元確認。
  - ◆ デジタル証明書とリンクした、より高機能な当人認証。
  - ◆ 属性によるアクセス認可。
- 実用化フェーズはまだこれからといったところ。証明書発行機関に関する規定や、暗号技術など様々な観点での標準化や制度化に関する課題がある。

CBDCにおける課題や論点

セコム IS研究所
Intelligent Systems Laboratory

- **標準化・ガイドライン**
  CBDCのユースケースやシステムモデルの整理に従い、認証手段・認証器に対する保証レベルの整理が必要。
  - 認証手段や認証器を（中央銀行、仲介機関、追加サービス）が提供するケース。既存の認証器を利用するケース。
  - 一本化した認証器を提供するケース、各社が独自に提供するケース、標準的な要件や仕様に準拠したものを提供するケース。
    - 認証器の一本化は不具合があった場合の影響が大きく、独自の場合には仕様の乱立の問題がある。標準化の場合には標準化体制の構築や既存の実装がある場合の移行計画等の課題がある。
  - 脆弱性が生まれやすい登録時（バインディング）に関するガイドラインの必要性。
- **プライバシー保護**
  消費者のプライバシー保護の観点とAMLの観点の両立。
  - モデルに応じて、中央銀行、仲介機関、追加サービスにおいてユーザー情報や利用履歴がどのように保存されるのか？それぞれの機関における情報保護の在り方。
  - 当人認証における識別子の設計。各事業者をまたがった追跡可能性。取引に関わるプライバシー保護と不正利用等があった場合の追跡可能性の在り方、設計方法。
- **短期的／中長期的な視点での技術動向の追従**
  直面したリスク（当人認証への新たな脅威など）へ対応する視点と、新たな技術動向（Identity Wallet等の例）を視野に入れた中長期的な導入・移行計画の検討が必要。情報共有・調査研究・計画立案の体制。

※ウォレットのハードウェアとしての議論は本WGのスコープ外であり、別のWGでカバーされる。

サマリ

認証を取り巻く状況

- 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン（デジタル庁）」やNIST SP 800-63等の改訂に加えて、マイナンバーカードやスマホの普及など、認証を取り巻く環境は変化。
- 銀行業界における当人認証の状況として、フィッシング被害が後を絶たない中、「フィッシング耐性」が、最近の至上命題。
- 2022年10月31日、米国CISAは「Implementing Phishing-Resistant MFA」ガイダンスを発表。
  ⇒フィッシング耐性のある認証方式は、「FIDO」か「公開鍵基盤(PKI)による多要素認証」

当行サービスにおけるフィッシング耐性

- ゆうちょ銀行では、FIDOを利用したゆうちょ認証アプリによりフィッシング耐性を確保。
- 犯人に狙われやすいFIDO登録（端末とアカウントの紐づけ）時においては、身元確認の手段であるeKYCを「口座保有者本人」による操作であることの確認にも活用し、フィッシング被害を防止。
- CBDCでは、「CBDC口座⇔銀行預金口座/決済アカウント」の連携が想定されるため、類似サービスとして、「即時振替サービス」を例に、連携元/連携先相互で実施している対策について紹介。

CBDCの検討課題と対応案

- CBDCの検討課題として、以下の観点について対応案を提示。
  - ガイドラインの整備の必要性
  - ガイドラインの見直し、位置づけ
  - 保証レベルとそれに応じた認証仕様統一化の必要性
  - その他規定すべきこと（設計段階からのセキュリティ考慮、ユニバーサルデザインを意識した認証、監視/モニタリングの必要性 等）